					Insira aqui a designação da entidade jurídica registada							
Número do documento: P26S					Título do documento: **Política de Segurança de Terceiros e Fornecedores**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	Controlos operacionais aplicáveis às relações com terceiros e fornecedores
ISO/IEC 27002:2022	Controlos 5.19–5.22	Controlos de segurança de fornecedores, termos contratuais de segurança, gestão de alterações, monitorização e revisão
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Aquisição, configuração, acordos de interligação e controlos aplicáveis a pessoal externo
RGPD da UE	Artigos 28, 32	Acordos de tratamento de dados e requisitos de segurança aplicáveis a subcontratantes
Diretiva NIS2 da UE	Artigos 21(2)(a)(b)(i), 23(1)	Gestão do risco da cadeia de abastecimento e supervisão de serviços prestados por terceiros
DORA da UE	Artigos 5(1)(2), 28(1)(2)	Gestão do risco das TIC aplicável a prestadores terceiros de serviços
COBIT 2019	APO10, APO12, DSS05	Gestão de fornecedores e integração do risco

1. Finalidade

1.1 Esta política estabelece os requisitos de segurança obrigatórios para a contratação, gestão e cessação de relações com terceiros e fornecedores que acedam aos dados, sistemas ou serviços da organização, ou que os possam afetar.

1.2 Assegura que prestadores externos — incluindo prestadores de suporte de TI, operadores de serviços cloud, programadores de software e prestadores de serviços de processos de negócio — tratam os ativos da empresa de forma segura e em conformidade com as leis e normas aplicáveis.

1.3 Esta política reduz riscos como fugas de dados, alterações não autorizadas aos sistemas, coimas regulatórias ou interrupções de negócio causadas por relações com terceiros inseguras ou insuficientemente governadas.

2. Âmbito

2.1 Esta política aplica-se a todos os terceiros que:

2.1.1 Prestem software, infraestrutura, serviços de alojamento ou serviços cloud

2.1.2 Acedam ou gerem sistemas, dispositivos ou aplicações internas

2.1.3 Tratem dados, documentos ou cópias de segurança da empresa

2.1.4 Apoiem operações de negócio, recursos humanos, finanças ou serviços ao cliente

2.2 Aplica-se igualmente a:

2.2.1 Colaboradores internos envolvidos na seleção, contratação ou supervisão de fornecedores

2.2.2 Qualquer elemento do pessoal que faça a gestão da integração de fornecedores, contratos, acessos ou revisões

2.2.3 Qualquer sistema ou processo dependente de componentes ou serviços de terceiros

3. Objetivos

3.1 Assegurar que todos os fornecedores cumprem requisitos de segurança claramente definidos.

3.2 Exigir que os contratos com fornecedores incluam obrigações vinculativas em matéria de segurança, privacidade e resposta a incidentes.

3.3 Avaliar e documentar os riscos dos fornecedores antes da celebração de acordos ou da concessão de acessos.

3.4 Realizar revisões regulares a fornecedores críticos ou de alto risco para confirmar a conformidade.

3.5 Estabelecer um processo formal para exceções, gestão de incidentes e atualização contratual.

3.6 Apoiar o cumprimento das obrigações da ISO/IEC 27001:2022, do RGPD da UE, da Diretiva NIS2 da UE e do DORA da UE relacionadas com a governação de fornecedores.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Detém a responsabilidade final pela seleção de fornecedores e pelo cumprimento dos requisitos de segurança

4.1.2 Aprova contratos, exceções e escalonamentos relacionados com fornecedores

4.1.3 Supervisiona a resposta a incidentes e a tomada de decisão quando os fornecedores não cumprem as suas obrigações

4.2 Prestador de serviços de TI ou contacto interno de segurança

4.2.1 Avalia o acesso técnico solicitado pelos fornecedores

4.2.2 Implementa regras de controlo de acessos, revê registos e verifica o tratamento seguro dos dados

4.2.3 Revê evidências de controlos de segurança, certificações ou resultados de auditoria, quando aplicável

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1 Esta política deve ser revista pelo menos anualmente pelo Diretor-Geral, com participação do prestador de serviços de TI ou do gestor do fornecedor.

9.2 A política deve também ser revista:

9.2.1 Após qualquer alteração significativa às obrigações legais, regulatórias ou contratuais

9.2.2 Na sequência de um incidente de segurança relacionado com um fornecedor ou de uma constatação de auditoria

9.2.3 Aquando da introdução de novas categorias de fornecedores (por exemplo, plataformas SaaS críticas)

9.3 Todas as atualizações devem ser:

9.3.1 Documentadas com histórico de versões e respetiva fundamentação

9.3.2 Aprovadas pelo Diretor-Geral

9.3.3 Comunicadas ao pessoal interno relevante e aos responsáveis pela gestão de fornecedores

9.3.4 Conservadas com as versões anteriores nos termos da P14S – Política de Retenção e Eliminação de Dados

10. Políticas relacionadas e articulações

10.1 A eficácia desta política depende da coordenação com as seguintes políticas de segurança da informação da PME:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: atribui a responsabilidade pela supervisão de fornecedores e pela execução contratual.

10.1.2 P4S – Política de Controlo de Acessos: define as regras de restrição de acesso que devem ser aplicadas quando são concedidos acessos a fornecedores.

10.1.3 P17S – Política de Proteção de Dados e Privacidade: assegura que os fornecedores que tratam dados pessoais cumprem os princípios de proteção de dados e os requisitos legais.

10.1.4 P14S – Política de Retenção e Eliminação de Dados: aplica-se a quaisquer dados ou registos partilhados com fornecedores ou por estes armazenados e rege a eliminação segura após a cessação do contrato.

10.1.5 P30S – Política de Resposta a Incidentes: define a forma de resposta quando um fornecedor causa ou está envolvido num incidente de segurança, incluindo procedimentos de escalonamento e tratamento de evidência.

10.2 Estas políticas funcionam em conjunto para assegurar que o risco associado a fornecedores é controlado ao longo de todo o ciclo de vida contratual.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Exige a implementação de controlos operacionais, incluindo os aplicáveis às relações com terceiros e fornecedores.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.19 – Assegura que as medidas de segurança dos fornecedores estão alinhadas com os requisitos da organização.

11.2.2 Controlo 5.20 – Exige acordos formais que abranjam termos de segurança, responsabilidades e obrigações em caso de violação.

11.2.3 Controlo 5.21 – Controla alterações aos serviços dos fornecedores que possam afetar a postura de segurança.

11.2.4 Controlo 5.22 – Exige a monitorização e revisão dos serviços dos fornecedores e da respetiva conformidade.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Regula a aquisição de sistemas e serviços externos, exigindo avaliações de risco e requisitos definidos.

11.3.2 SA-10 – Controla procedimentos de configuração e alteração que envolvam sistemas geridos por terceiros.

11.3.3 CA-3 – Exige acordos de interligação para sistemas que envolvam entidades externas.

11.3.4 PS-7 – Especifica verificação e responsabilização aplicáveis a pessoal externo.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 28 – Exige acordos de tratamento de dados com fornecedores que atuem como subcontratantes.

11.4.2 Artigo 32 – Impõe medidas técnicas e organizativas de segurança adequadas a todos os subcontratantes.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(a), (b), (i) – Impõe a gestão do risco da cadeia de abastecimento das TIC e controlos sobre terceiros.

11.5.2 Artigo 23(1) – Exige supervisão documentada dos serviços prestados por terceiros para entidades essenciais e importantes.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 5(1) – Exige um quadro de gestão do risco das TIC que abranja todos os prestadores terceiros críticos.

11.6.2 Artigo 5(2) – Estabelece controlos contratuais e operacionais para dependências de serviços de TIC.

11.6.3 Artigo 28(1), (2) – Estabelece regras de supervisão para o risco associado a terceiros prestadores de serviços de TIC no setor financeiro.

11.7 COBIT 2019

11.7.1 APO10 – “Manage Suppliers” define controlos de aprovisionamento e expectativas de gestão da relação.

11.7.2 APO12 – “Manage Risk” integra o risco de fornecedores na governação do risco da organização.

11.7.3 DSS05 – “Manage Security Services” aplica-se a prestadores terceiros de serviços geridos e a prestadores de serviços externalizados.